INFORMATION-PRESERVING SYSTEM, INFORMATION MOVING SYSTEM AND STORAGE MEDIUM USED FOR THEM

Patent number: JP2002101087

Publication date: 2002-04-05

Inventor: ASAHI TAKESHI; KAWASAKI IKUYA; KITAHARA JUN; MIZUSHIMA EIGA; OWADA TORU; TAMURA TAKAYUKI; TOTSUKA TAKASHI

Applicant: HITACHI LTD

Classification:

- international: H04L9/10; G06F12/14; H04L9/08

- european:

Application number: JP20000286479 20000921

Priority number(s): JP20000286479 20000921

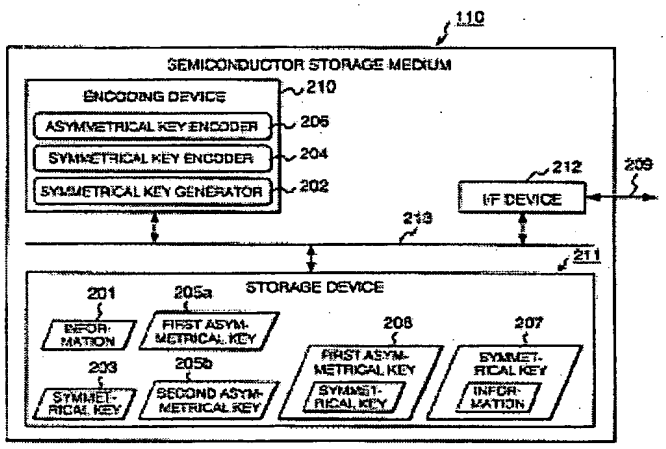
Also published as:

US2002034306 (A1)

Abstract not available for JP2002101087

Abstract of corresponding document: **US2002034306**

A storage medium and an information processing system utilizing that storage medium capable of outputting information stored on the storage medium in a format unusable by other information devices or storage mediums. A storage medium and an information processing system utilizing that storage medium further capable of transferring information stored on the storage medium rather than copying the information so that the uniqueness of the information is assured. A storage medium comprised of a storage device for storing information, information required for encryption and encrypted information, and an I/F device for inputting and outputting information, information required for coding and store encrypted information in a storage device or from an external apparatus other than the storage device, and an encoding device for coding of information and decoding of encoded information. When outputting information stored inside the storage device to outside the storage medium, information is encoded using encryption key information, and along with obtaining the encoded information and obtaining the encoded encryption key information by using another encryption information, both the encoded information and encoded encryption key information are output so that decoding the information without the storage medium is impossible



(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号
特開2002－101087
（P2002－101087A）
(43)公開日　平成14年４月５日(2002.4.5)

(51)Int.Cl.[7]	識別記号	Ｆ Ｉ		テーマコード（参考）
Ｈ０４Ｌ　9/10		Ｇ０６Ｆ　12/14	３２０Ｂ	５Ｂ０１７
Ｇ０６Ｆ　12/14	３２０		３２０Ｅ	５Ｊ１０４
		Ｈ０４Ｌ　9/00	６２１Ａ	
Ｈ０４Ｌ　9/08			６０１Ｃ	
			６０１Ｅ	

審査請求　未請求　請求項の数５　ＯＬ　（全 14 頁）

(21)出願番号　特願2000－286479(P2000－286479)

(22)出願日　平成12年９月21日(2000.9.21)

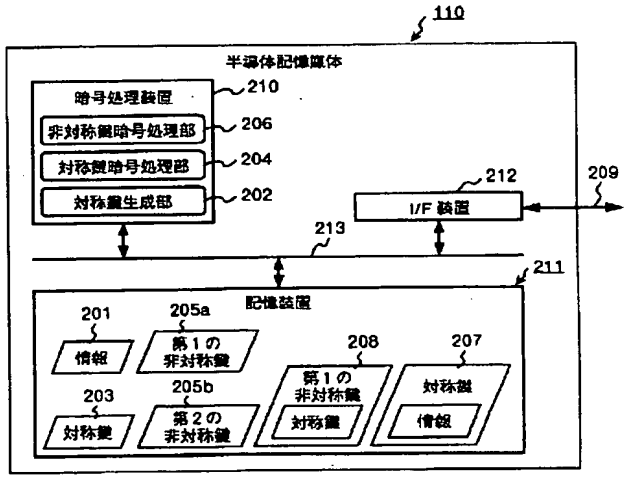
(71)出願人　000005108
株式会社日立製作所
東京都千代田区神田駿河台四丁目６番地
(72)発明者　大和田　徹
神奈川県川崎市麻生区王禅寺1099番地　株式会社日立製作所システム開発研究所内
(72)発明者　北原　潤
神奈川県川崎市麻生区王禅寺1099番地　株式会社日立製作所システム開発研究所内
(74)代理人　100068504
弁理士　小川　勝男　（外２名）

最終頁に続く

(54)【発明の名称】　情報保管システム及び情報移動システム並びにそれらに用いる記憶媒体

(57)【要約】　（修正有）
【課題】　記憶媒体に格納されている情報を他の情報機器又は記憶媒体で使用することが不可能な形式で出力し、該情報を複製ではなく移動して、情報の唯一性を保証する記憶媒体及び情報処理システムを提供する。
【解決手段】　記憶媒体１１０は、情報、暗号処理に必要な情報、及び暗号化された情報を保管する記憶装置２１１と保管された上記情報を記憶媒体以外の外部機器から入力し、且つ出力するＩ／Ｆ装置２１２、及び、情報に対する暗号化、復号化を行なう暗号処理装置２１０を備え、更に、保管した情報を記憶媒体外に出力する時に、該情報に暗号鍵情報を用いた暗号化情報を得ると共に、該情報を暗号化する際に用いた暗号鍵情報を、該暗号鍵情報とは独立の、該暗号鍵情報を暗号化する際に用いる暗号鍵情報を用いて暗号化し、暗号化暗号鍵情報を得、該暗号化情報と該暗号化暗号鍵情報を共に出力することで、該記憶媒体以外では該情報を復号化することを困難とする。

図　2



1

【特許請求の範囲】

【請求項１】情報、暗号処理に必要な暗号処理鍵、及び暗号化された暗号化情報を保管する記憶装置と、該記憶装置に保管された該情報、該暗号処理鍵、又は該暗号化情報の入出力を行う入力装置と、該情報に対する暗号処理、該暗号化情報に対する復号処理を行なう暗号処理装置とを備え、

該記憶装置内に保管した情報を記憶媒体外に出力する場合には、該情報を該暗号処理鍵を用いて暗号化した該暗号化情報を得ると共に、該情報を暗号化する際に用いた該暗号処理鍵を、他の暗号処理鍵を用いて暗号化した暗号化暗号処理鍵を得、該暗号化情報と該暗号化暗号処理鍵を共に出力するように構成されることを特徴とする記憶媒体。

【請求項２】情報、暗号処理に必要な暗号処理鍵、及び暗号化された暗号化情報を保管する記憶装置と、該記憶装置に保管された、該情報、該暗号処理鍵、又は該暗号化情報の入出力を行う入力装置と、該情報に対する暗号処理、該暗号化情報に対する復号処理を行なう暗号処理装置とを備え、

該記憶装置内に保管した情報を記憶媒体外に出力する場合には、該情報を該暗号処理鍵を用いて暗号化して該暗号化情報を得ると共に、該情報を暗号化する際に用いた該暗号処理鍵を、他の暗号処理鍵を用いて暗号化した暗号化暗号処理鍵を得、先ず、該暗号化情報のみを出力し、外部機器から該暗号化情報が入力されたことを示す信号が入力された時、該記憶装置に保管された情報を無効化した後、該暗号化暗号処理鍵を出力するように構成されることを特徴とする記憶媒体。

【請求項３】請求項１又は２記載の記憶媒体において、該記憶媒体の有する入力装置、該暗号処理装置及び該記憶装置が同一の半導体チップ上に構成されることを特徴とする記憶媒体。

【請求項４】情報、暗号処理に必要な暗号処理鍵、及び暗号化された暗号化情報を保管する記憶装置、該記憶装置に保管された、該情報、該暗号処理鍵、又は該暗号化情報の入出力を行う入力装置、該情報に対する暗号処理、該暗号化情報に対する復号処理を行なう暗号処理装置を有する記憶媒体と、

該記憶媒体と接続される外部装置と、を備え、

該情報を該暗号処理鍵を用いて暗号化して得た該暗号化情報と、該情報を暗号化する際に用いた該暗号処理鍵を、他の暗号処理鍵を用いて暗号化した暗号化暗号処理鍵とを該外部装置に転送して記憶することを特徴とする情報保管システム。

【請求項５】情報、暗号処理に必要な暗号処理鍵、及び暗号化された暗号化情報を保管する記憶装置、該記憶装置に保管された、該情報、該暗号処理鍵、又は該暗号化情報の入出力を行う入力装置、該情報に対する暗号処理、該暗号化情報に対する復号処理を行なう暗号処理装置を有する記憶媒体と、

該記憶媒体に記憶された情報を受信する外部装置と、を備え、

該情報を該外部装置に転送する場合には、該情報を該暗号処理鍵を用いて暗号化して得た該暗号化情報を該外部装置に転送し、該外部装置から該暗号化情報を受信したことを示す信号を受信した後、該記憶装置に保管された情報を無効化し、該暗号化暗号処理鍵を該外部装置に転送することを特徴とする情報移動システム。

2

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、情報を半導体記憶媒体で流通させる場合の情報保管システム及び情報移動システム並びにこれらに用いる記憶媒体に係り、特に、付加価値の高い情報を、複製による不正使用を防ぎながら、例えばＰＣ向けの大容量磁気記憶装置など特に情報の複製防止機能を具備していない汎用の情報記憶媒体に保管する方法及び同情報を記憶媒体間での複製を許さずに移動する方法に関する。

【０００２】

【従来の技術】従来の付加価値の高い情報を、複製による不正使用を防ぎながら流通させる方式として、特開２０００－９００３９号公報に記載されているようなシステムがある。図９を用いて同装置の動作を簡単に説明する。図９は従来の複製による不正使用防止システムを示すブロック図である。同システムでは、音楽サーバ９０３とクライアント９０２がインターネット９０１で接続されている。クライアント９０２において、再生装置９１１固有のＩＤに基づき公開鍵及び秘密鍵が作成される。公開鍵は、パーソナルコンピュータ９０２からサーバ９０３に送られ、登録される。秘密鍵は、装置９１１に保持される。クライアント９０２からサーバ９０３に対して、音楽データの配信が要求される。音楽ＤＢ９２２から取り出された音楽データに対して、登録された公開鍵で暗号化が施される。暗号化された音楽データがクライアント９０２に送信され、再生装置９１１に保存される。再生時には、再生装置９１１に保持された秘密鍵で音楽データが復号化されながら再生される。再生装置９１１に保存された音楽データは、再生装置９１１固有のＩＤに基づき作成された鍵で暗号化されているため、他の再生装置では再生できない。

【０００３】又、従来の付加価値の高い情報を、記憶媒体間での複製を許さずに移動する方式として、特開平１１－２５９９６４号公報に記載されているような装置がある。図１０を用いて同装置の動作を簡単に説明する。図１０は従来の情報移動システムのフローチャートである。同装置では、移動によってデータを移動先に複製すると、移動元のデータは、再生が禁止される。移動先の機器には、予め固有の識別子が設定される。ステップ１０５０で移動元機器に移動先機器が接続されると、ステ

ップ１０５１で移動先機器から識別子が送信される。移動先では、ステップ１０５２で、予め登録された識別子管理表から送信された識別子が探され、ステップ１０５３でこの識別子が見つかったか、見つからなかったかを判断する。見つからなければステップ１０６１に移行し、移動が禁止される。ステップ１０５３で識別子が見つかれば、ステップ１０５４で曲の選択が行われ、移動の指示がなされる。次に、ステップ１０５５で移動元でデータ管理表から移動するデータが探され、ステップ１０５６でフラグが調べられる。ステップ１０５７でフラグが‘１’であれば、ステップ１０６１に移行して、そのデータが既に移動されたとして移動が禁止される。フラグが‘０’であれば、ステップ１０５８で、データが移動され、ステップ１０５９で、データ管理表が更新される。

【０００４】

【発明が解決しようとする課題】従来、半導体記憶媒体に格納された情報は、他の半導体記憶媒体への複製が容易に行なえるため、情報に付加価値をつけることが困難であるという問題があった。逆に言えば、付加価値の高いデータは、簡単に複製されてしまうのを防止するために半導体記憶媒体で流通させることは行わなれてこなかった。これに対し、従来の付加価値の高い情報を、複製による不正使用を防ぎながら流通させる方式では、サーバ９０３が、付加価値の高い情報を、再生装置９１１固有のＩＤに基づき暗号化するため、通信系路上で同情報を盗聴し不正に利用することを防止することが可能である。

【０００５】又、転送元機器から転送先機器に暗号化情報を渡す際、「例えば音楽データなどの高付加価値情報を、共通鍵暗号方式で暗号化して転送する。」「上記暗号化に用いた共通鍵を、公開鍵暗号方式で暗号化して転送する。」と言った二段に鍵を組み合わせた暗号化は処理速度、鍵管理の容易性から一般的である。ここで、後者の暗号化は、転送先機器で復号可能な暗号鍵を用いている（鍵の共有を行なっている）ことから、転送先機器で有価値情報を利用することが可能となっている。

【０００６】又、従来の付加価値の高い情報を、記憶媒体間での複製を許さずに移動する方式では、データの複製許可／不許可フラグとデータ複製後のデータ移動元でのデータ再生禁止機能を設けることで、付加価値の高い情報の移動を実現している。しかし、同方式においては情報の移動元、移動先間の通信経路の保護が十分でなく同通信経路上の盗聴で、付加価値の高い情報の不正な取得を許してしまう可能性がある。又、一連の移動処理途上で、データ移動元、移動先に利用可能なデータが存在する時点がありデータ移動元、移動先間の通信遮断などによりデータ移動元、移動先のデータが共に利用可能となってしまう可能性がある。

【０００７】本発明の目的は上記問題点を解決するためになされたものであり、記憶媒体自体への機能追加により、同記憶媒体に格納されている情報を他の情報機器又は記憶媒体で使用することが不可能な形式で出力する（鍵を共有しない）ことが可能な記憶媒体及びそれを用いた情報処理技術を提供することにある。更に、本発明の他の目的は記憶媒体に格納されている情報を、通信経路上の盗聴による複製を防止しつつ、複製ではなく移動することで、常に情報の唯一性を保証することが可能な記憶媒体及びそれを用いた情報処理技術を提供することにある。

【０００８】

【課題を解決するための手段】本発明の目的を達成するために、第１の発明では、記憶媒体は、情報、暗号処理に必要な暗号処理鍵、及び暗号化された暗号化情報を保管する記憶装置と、該記憶装置に保管された該情報、該暗号処理鍵、又は該暗号化情報の入出力を行う入力装置と、該情報に対する暗号処理、該暗号化情報に対する復号処理を行なう暗号処理装置とを備え、該記憶装置内に保管した情報を記憶媒体外に出力する場合には、該情報を該暗号処理鍵を用いて暗号化した該暗号化情報を得ると共に、該情報を暗号化する際に用いた該暗号処理鍵を、他の暗号処理鍵を用いて暗号化した暗号化暗号処理鍵を得、該暗号化情報と該暗号化暗号処理鍵を共に出力するように構成される。

【０００９】第２の発明では、記憶媒体は、情報、暗号処理に必要な暗号処理鍵、及び暗号化された暗号化情報を保管する記憶装置と、該記憶装置に保管された、該情報、該暗号処理鍵、又は該暗号化情報の入出力を行う入力装置と、該情報に対する暗号処理、該暗号化情報に対する復号処理を行なう暗号処理装置とを備え、該記憶装置内に保管した情報を記憶媒体外に出力する場合には、該情報を該暗号処理鍵を用いて暗号化して該暗号化情報を得ると共に、該情報を暗号化する際に用いた該暗号処理鍵を、他の暗号処理鍵を用いて暗号化した暗号化暗号処理鍵を得、先ず、該暗号化情報のみを出力し、外部機器から該暗号化情報が入力されたことを示す信号が入力された時、該記憶装置に保管された情報を無効化した後、該暗号化暗号処理鍵を出力するように構成される。

【００１０】第１または第２の発明において、該記憶媒体の有する入力装置、該暗号処理装置及び該記憶装置が同一の半導体チップ上に構成される。

【００１１】第３の発明では、情報保管システムは、情報、暗号処理に必要な暗号処理鍵、及び暗号化された暗号化情報を保管する記憶装置、該記憶装置に保管された、該情報、該暗号処理鍵、又は該暗号化情報の入出力を行う入力装置、該情報に対する暗号処理、該暗号化情報に対する復号処理を行なう暗号処理装置を有する記憶媒体と、該記憶媒体と接続される外部装置とを備え、該情報を該暗号処理鍵を用いて暗号化して得た該暗号化情報と、該情報を暗号化する際に用いた該暗号処理鍵を、

他の暗号処理鍵を用いて暗号化した暗号化暗号処理鍵とを該外部装置に転送して記憶する。

【００１２】第４の発明では、情報移動システムは、情報、暗号処理に必要な暗号処理鍵、及び暗号化された暗号化情報を保管する記憶装置、該記憶装置に保管された、該情報、該暗号処理鍵、又は該暗号化情報の入出力を行う入力装置、該情報に対する暗号処理、該暗号化情報に対する復号処理を行なう暗号処理装置を有する記憶媒体と、該記憶媒体に記憶された情報を受信する外部装置とを備え、該情報を該外部装置に転送する場合には、該情報を該暗号処理鍵を用いて暗号化して得た該暗号化情報を該外部装置に転送し、該外部装置から該暗号化情報を受信したことを示す信号を受信した後、該記憶装置に保管された情報を無効化し、該暗号化暗号処理鍵を該外部装置に転送する。

【００１３】

【発明の実施の形態】以下、本発明の実施の形態について、幾つかの実施例を用い、図を参照して説明する。図１は本発明を適用することができる情報処理システムの一実施例の概要を示すブロック図である。図に示すように、情報処理システムは、情報を生成する情報生成者および情報生成装置１０１と、転送手段１０２を介して接続された、情報配信装置１０３と、情報配信装置１０３と通信回線１０４で接続された、少なくとも１台の専用情報処理装置１０５と、少なくとも１個の半導体記憶媒体１１０と、少なくとも１台の情報再生装置１０９からなる。

【００１４】専用情報処理装置１０５以外に、通信回線１０４に接続可能な、半導体記憶媒体アクセス手段１０７を備えた、パーソナルコンピュータ等の汎用情報処理装置１０６と、情報再生装置１０８が存在しても良い。情報は、情報生成者および情報生成装置１０１で生成され、情報配信装置１０３内に格納される。この時の情報の転送には、通信回線を用いても良いし、フロッピー（登録商標）ディスク等の磁気記憶媒体を介して、転送されても良い。情報配信装置１０３は、同装置に格納された情報を、専用情報処理装置１０５、汎用情報処理装置１０６、情報再生装置１０８からの要求に応じて、情報を加工し、または補助情報を付加し、通信回線１０４を介して転送する。

【００１５】情報を転送された専用情報処理装置１０５、汎用情報処理装置１０６、情報再生装置１０８は、接続されている半導体記憶媒体１１０に、情報を転送する。専用情報処理装置１０５は、複数の情報を蓄積しておき、専用情報処理装置１０５で情報の加工および補助情報の付加の処理を行っても良い。汎用情報処理装置１０６、情報再生装置１０８は、情報配信装置１０３から転送された情報を基本的にそのまま半導体記憶媒体１１０に転送する。このとき、情報配信装置１０３と専用情報処理装置１０５間、専用情報処理装置１０５と半導体

記憶媒体１１０間、情報配信装置１０３と半導体記憶媒体１１０間ではそれぞれを認識し正当性を判断する情報交換を行う。

【００１６】加工または補助情報を付加された配信情報を格納した半導体記憶媒体１１０は、情報再生装置１０９に接続され、情報再生装置１０９からの要求に応じて、格納してある情報を転送する。このとき、半導体記憶媒体１１０と、情報再生装置１０９とを認識し正当性を判断する情報交換を行う。

【００１７】尚、情報生成者及び情報生成装置１０１が生成した情報を半導体記憶媒体１１０に安全に配信する方法は、本発明では特に言及せず、半導体記憶媒体１１０には配信された情報が格納されていることを前提とする。

【００１８】以下、本発明の第１の実施例について、図２～図４、及び図８を用いて説明する。図２は本発明による記憶媒体の第１の実施例を示す構成図であり、半導体記憶媒体１１０は主に暗号処理装置２１０と記憶装置２１１及びＩ／Ｆ装置２１２から構成される。図において、暗号処理装置２１０は、非対称鍵暗号や公開鍵暗号と呼ばれる、暗号鍵と復号鍵が異なる暗号方式を用いた暗号処理を行う非対称鍵暗号処理部２０６と、対称鍵暗号や共通鍵暗号と呼ばれる、暗号鍵と復号鍵が同じである暗号方式を用いた暗号処理である対称鍵暗号処理２０４と、何らかの乱数生成処理を用いた対称鍵生成処理２０２などから構成される。記憶装置２１１は、情報２０１、対称鍵２０３、第１の非対称鍵２０５ａ、第２の非対称鍵２０５ｂ、第１の非対称鍵で暗号化された対称鍵２０８、対称鍵で暗号化された情報２０７などを保管する。インターフェース装置２１２（以下、Ｉ／Ｆ装置と言う）は、半導第記憶媒体１１０と外部機器との間の情報のやり取りを制御する。データバス２１３は、暗号処理装置２１０、記憶装置２１１、Ｉ／Ｆ装置２１２間で情報、制御信号をやり取りする。また、データバス２０９は半導第記憶媒体１１０と外部機器間で情報、制御信号をやり取りする。

【００１９】半導体記憶媒体１１０にはあらかじめ記憶媒体固有情報を記録しておく。すなわち、記憶装置２１１には、半導体記憶媒体１１０固有の第１の非対称鍵２０５ａと第２の非対称鍵２０５ｂの２つが記憶される。固有情報を設定するには、半導体記憶媒体１１０を製造する段階で書き込み、半導体記憶媒体１１０が完成してからは容易に書き換えることが不可能な方式をとってもよいし、製造管理者など限定され、かつ情報の管理が十分に行なえる範囲にのみ公開される方式を用いて、半導体記憶媒体１１０の完成後に、固有情報を設定する方式をとってもよい。

【００２０】この半導体記憶媒体１１０固有の第１、第２の非対称鍵２０５ａ、２０５ｂは非対称鍵暗号や公開鍵暗号と呼ばれる方式の鍵データである。非対称鍵暗号

や公開鍵暗号と呼ばれる暗号方式は、平文を第１の非対称鍵を暗号鍵として暗号化し暗号文を生成すると、暗号文は第２の非対称鍵を復号鍵としてのみ復号が可能となり、平文を第２の非対称鍵を暗号鍵として暗号化し暗号文を生成すると、暗号文は第１の非対称鍵を復号鍵としてのみ復号が可能となるという特徴を持つ暗号方式である。以下では、第１の非対称鍵を公開鍵、第２の非対称鍵を秘密鍵として用いる。また、２０７は対称鍵を用いて暗号化された情報である暗号化情報を意味し、２０８は非対称鍵を用いて対称鍵を暗号化された対称鍵である暗号化対称鍵を意味する。

【００２１】次に、図３及び図８（ａ）を用いて、本実施例に掛かる半導第記憶媒体１１０に保管された情報２０１を汎用情報処理装置１０６及び半導体記憶媒体アクセス手段１０７へ情報２０１を転送する場合の手順を説明する。図３は本発明による情報移動システムの記憶媒体からの情報転送機能の第１の実施例を示す図であり、図８（ａ）、（ｂ）は図３の情報移動システムの動作を説明するためのフローチャートであり、（ａ）は半導体記憶媒体１１０からの情報転送の動作を示し、（ｂ）は半導体記憶媒体１１０への情報転送を示す。

【００２２】半導体記憶媒体１１０に接続された汎用情報処理装置１０６及び半導体記憶媒体アクセス手段１０７による情報２０１の転送要求に応じて、半導体記憶媒体１１０は以下の動作を行う。

【００２３】図２、図３および図８を参照して説明すると、ステップ２０２で、半導体記憶媒体１１０は暗号処理装置２１０の機能によって乱数を生成する。生成された乱数は情報２０１を暗号化する対称鍵２０３として用いられる。ステップ２０４ａで、情報２０１は、暗号処理装置２１０の機能によって、対称鍵２０３を暗号鍵とした対称鍵暗号化が施され、暗号化情報２０７が生成される。一方、対称鍵２０３は、ステップ２０６ａに示すように、暗号処理装置２１０の機能によって、第１の非対称鍵２０５ａを暗号鍵として、非対称暗号化が施され、暗号化対称鍵２０８が生成される。

【００２４】上記手順により生成された暗号化情報２０７及び暗号化対称鍵２０８は、Ｉ／Ｆ装置２１２の機能によって、ステップ２０９ａで、汎用情報処理装置１０６及び半導体記憶媒体アクセス手段１０７に転送される。これによって、暗号化情報２０７及び暗号化対称鍵２０８は汎用情報処理装置１０６及び半導体記憶媒体アクセス手段１０７にバックアップ用として保管することができる。

【００２５】上記手順によって汎用情報処理装置１０６及び半導体記憶媒体アクセス手段１０７に転送された暗号化情報２０７は、対称鍵２０３がないと正当に復号できない。又、暗号化対称鍵２０８は、第２の非対称鍵２０５ｂがないと正当に復号できない。ここで、第２の非対称鍵２０５ｂは、半導体記憶媒体１１０固有の鍵データであり、汎用情報処理装置１０６及び半導体記憶媒体アクセス手段１０７はこれを得ることができない。従って、該汎用情報処理装置１０６及び半導体記憶媒体アクセス手段１０７は、暗号化対称鍵２０８を復号して情報２０１を利用することができない。

【００２６】つまり、半導体記憶媒体１１０上に保管された情報２０１は、汎用情報処理装置１０６及び半導体記憶媒体アクセス手段１０７に転送された後、汎用情報処理装置１０６などの機能によってその複製を作成されることがあっても、該複製情報は汎用情報処理装置１０６及び半導体記憶媒体アクセス手段１０７上では使用不可能である、このことから、汎用情報処理装置１０６での情報２０１の無制限な複製を防ぐことが可能である。

【００２７】又、転送されるべき情報２０１を暗号化するため用いた対称鍵２０３は、情報２０１の復号のために必須であるため、本来は半導体記憶媒体１１０内に転送される情報毎に管理、保管されるべきであるが、本実施例に係る半導体記憶媒体１１０は、対称鍵２０３を半導体記憶媒体１１０固有の第１の非対称鍵２０５ａで暗号化された暗号化対称鍵２０８とし、ステップ２０９ａで暗号化情報２０７と共に、半導体記憶媒体１１０外に転送される。このことにより、半導体記憶媒体１１０内で複数の対称鍵を管理、保管する必要がなくなるので、第１及び第２の非対称鍵ペア２０５ａ、２０５ｂのみ管理、保管すればよい。すなわち、鍵管理が容易となると共に複数の対称鍵データによって記憶装置２１１の記憶容量を占有しないという利点がある。

【００２８】次に、図４及び図８（ｂ）を用いて、図３に示した手順によって汎用情報処理装置１０６及び半導体記憶媒体アクセス手段１０７へ転送された暗号化情報２０７を、半導体記憶媒体１１０へ転送する場合の手順を説明する。

【００２９】図４は本発明による情報移動システムの記録媒体への情報転送機能の第１の実施例を示す図である。半導体記憶媒体１１０に接続された汎用情報処理装置１０６及び半導体記憶媒体アクセス手段１０７による情報２０１の転送要求に応じて、半導体記憶媒体１１０は以下の動作を行う。半導体記憶媒体１１０は、ステップ２０９ｂにおいて、Ｉ／Ｆ装置２１２の機能によって汎用情報処理装置１０６及び半導体記憶媒体アクセス手段１０７から暗号化情報２０７及び暗号化対称鍵２０８を入力する。次に、半導体記憶媒体１１０は、ステップ２０６ｂで、暗号処理装置２１０の機能によって第２の非対称鍵２０５ｂを復号鍵として暗号化対称鍵２０８に非対称復号化を施し、対称鍵２０３を得る。更に、ステップ２０４ｂで、暗号処理装置２１０の機能によって上記手順で得られた対称鍵２０３を復号鍵として暗号化情報２０７に対称鍵復号化を施し、情報２０１を得る。

【００３０】ここで、第２の非対称鍵２０５ｂは、半導体記憶媒体１１０固有の鍵データであることから、汎用

情報処理装置１０６及び半導体記憶媒体アクセス手段１０７に転送された暗号化情報２０７は、暗号化情報２０７の転送元となった同一の半導体記憶媒体１１０でのみ復号可能である。このことから、汎用情報処理装置１０６及び半導体記憶媒体アクセス手段１０７に転送された暗号化情報２０７を転送元となった半導体記憶媒体１１０以外の半導体記憶媒体に転送して復号、使用することは不可能であり、情報２０１の無制限な複製を防ぐことが可能である。

【００３１】以上、本実施例における半導体記憶媒体によれば、通信系路上での盗聴による情報の不正取得を防止する目的で複数の機器間で暗号通信を行い、転送元機器から転送先機器に情報を渡す際に、「音楽データなどの高付加価値情報を暗号化して転送する」、「上記暗号化に用いた鍵を、別の鍵で暗号化して転送する」と言った二段に鍵を組み合わせた暗号化を行なうことができる。但し、後者の暗号化は、転送先機器では復号不可能な暗号鍵を用いている（鍵を共有していない）ことから、転送先機器で、暗号化された有価値情報を復号し、利用することは不可能となっており、転送元機器に同情報を書き戻した際にのみ利用可能となる。又、高付加価値情報の暗号化に用いる鍵を固定とすることは暗号解読の有力な手掛りを与えることとなり安全上問題があるため、同鍵は、擬似乱数生成器などにより暗号通信が必要となるたびに生成する。転送先機器は、高付加価値情報を暗号化するために生成した鍵を、転送先機器でしか復号できない形に暗号化して高付加価値情報と共に出力してしまうために、鍵管理が容易となり（唯一の鍵のみ管理）、且つ、複数の鍵情報によって記憶容量を圧迫されることがない。

【００３２】すなわち、本実施例における半導体記憶媒体によれば、付加価値の高い情報を、複製による不正使用を防ぎながら、例えばＰＣ向けの大容量磁気記憶装置など、特に情報の複製防止機能を具備していない汎用の情報記憶媒体に保管することが可能である。

【００３３】次に、本発明の第２の実施例について、図５及び図６を用いて説明する。図５は本発明による情報管理及び移動システムの概略構成図、図６は本発明による情報移動システムの第２の実施例の動作を示すフローチャートである。図５では、本実施例に係る半導体記憶媒体１１０ａ及び１１０ｂと同媒体制御装置（専用情報処理装置１０５、又は汎用情報処理装置１０６及び半導体記憶媒体アクセス手段１０７、又は再生装置１０８）の概略構成を示す。

【００３４】図中、情報２０１、対称鍵生成部２０２、対称鍵２０３、対称鍵暗号処理部２０４、非対称鍵暗号処理部２０６、データバス２０９、暗号処理装置２１０、記憶装置２１１、Ｉ／Ｆ装置２１２及びデータバス２１３は、第１の実施例に示したものと同様のものである。

【００３５】１１０ａは情報２０１の転送元となる半導体記憶媒体、１１０ｂは、情報２０１の転送先となる半導体記憶媒体である。２０５ａはあらかじめ情報転送元半導体記憶媒体１１０ａの記憶装置２１１に保管された、情報転送先半導体記憶媒体１１０ｂの非対称暗号方式を用いた公開鍵（以下、第１の非対称鍵）、２０５ｂはあらかじめ情報転送先半導体記憶媒体１１０ｂの記憶装置２１１に保管された、情報転送先半導体記憶媒体１１０ｂの非対称暗号方式を用いた秘密鍵（以下、第２の非対称鍵）である。

【００３６】５０１ａ、５０１ｂは専用情報処理装置１０５、又は汎用情報処理装置１０６及び半導体記憶媒体アクセス手段１０７、又は再生装置１０８との間の情報、制御信号のやり取りを制御するインターフェース装置（以下、Ｉ／Ｆ装置）である。

【００３７】５０２は一方のＩ／Ｆ装置５０１ａを介して入力した情報を他方のＩ／Ｆ装置５０１ｂを介して出力するように制御してなる制御回路である。５０３ａ、５０３ｂはＩ／Ｆ装置５０１と制御回路５０２間で情報、制御信号をやり取りするデータバスである。

【００３８】次に、図６を用いて、情報転送元半導体記憶媒体１１０ａに保管された情報２０１を専用情報処理装置１０５、又は汎用情報処理装置１０６及び半導体記憶媒体アクセス手段１０７、又は情報再生装置１０８を介して、情報転送先半導体記憶媒体１１０ｂへ転送する場合の手順を説明する。

【００３９】情報転送元半導第記憶媒体１１０ａに接続された専用情報処理装置１０５、又は汎用情報処理装置１０６及び半導体記憶媒体アクセス手段１０７、又は情報再生装置１０８による情報２０１の転送要求に応じて、情報転送元半導第記憶媒体１１０ａ及び情報転送先半導第記憶媒体１１０ｂは以下の動作を行う。

【００４０】図６において、ステップ６０１で、情報転送元半導第記憶媒体１１０ａは対称鍵を生成する。即ち、暗号処理装置２１０の機能によって乱数を生成し、生成された乱数は情報２０１を暗号化する対称鍵２０３として用いられる。ステップ６０２で、情報２０１は、暗号処理装置２１０の機能によって、対称鍵２０３を暗号鍵とした対称鍵暗号化を施され、暗号化情報２０７が生成される。上記手順により生成された暗号化情報２０７は、ステップ６０３ａにおいて、Ｉ／Ｆ装置２１２の機能によって、専用情報処理装置１０５、又は汎用情報処理装置１０６及び半導体記憶媒体アクセス手段１０７、又は再生装置１０８を介して、情報転送先半導第記憶媒体１１０ｂに送信される。

【００４１】情報転送先半導第記憶媒体１１０ｂは、ステップ６０３ｂで、暗号化情報２０７を受信し、ステップ６０４で受信した暗号化情報２０７の転送誤りをチェックする。もし転送誤りがあれば、情報転送先半導第記憶媒体１１０ｂは、ステップ６０５ａで情報転送元半導

第記憶媒体１１０ａに対し情報再送要求を送信する。情報転送元半導第記憶媒体１１０ａは、ステップ６０５ｂで、情報再送要求を受信し、ステップ６０３ａで再度、暗号化情報を送信する。もし転送誤りがなければ、情報転送先半導第記憶媒体１１０ｂは、ステップ６０６ａで情報転送元半導第記憶媒体１１０ａに対し情報受信完通知を送信する。

【００４２】情報転送元半導第記憶媒体１１０ａは、ステップ６０６ｂで情報受信完通知を受信し、ステップ６０７で情報２０１の削除動作を行う。この削除動作は、Ｉ／Ｆ装置２１２を介して外部からデータアクセスが不可能となることを保証可能であるならば、記憶装置２１１上からの物理的なデータ消去を伴わなくともよい。

【００４３】次に、ステップ６０８で、情報転送元半導第記憶媒体１１０ａは、暗号処理装置２１０の機能によって、対称鍵２０３に第１の非対称鍵２０５ａを暗号鍵とした非対称暗号化を施し、暗号化対称鍵２０８を生成する。上記手順により生成された暗号化対称鍵２０８は、ステップ６０９ａで、Ｉ／Ｆ装置２１２の機能によって、専用情報処理装置１０５、又は汎用情報処理装置１０６及び半導体記憶媒体アクセス手段１０７、又は情報再生装置１０８を介して、情報転送先半導第記憶媒体１１０ｂに送信される。

【００４４】情報転送先半導第記憶媒体１１０ｂは、ステップ６０９ｂで暗号化対称鍵２０８を受信し、ステップ６１０で受信した暗号化対称鍵２０８の転送誤りをチェックする。もし転送誤りがあれば、ステップ６１１ａで情報転送先半導第記憶媒体１１０ｂは、情報転送元半導第記憶媒体１１０ａに対し対称鍵再送要求を送信する。情報転送元半導第記憶媒体１１０ａは、ステップ６１１ｂで対称鍵再送要求を受信し、ステップ６０９ａに戻り、再度、暗号化対称鍵を送信する。もし転送誤りがなければ、情報転送先半導第記憶媒体１１０ｂは、ステップ６１２で暗号処理装置２１０の機能によって、暗号化対称鍵２０８に第２の非対称鍵２０５ｂを暗号鍵とした非対称復号化を施し、対称鍵２０３を生成する。次に、ステップ６１３で情報転送先半導第記憶媒体１１０ｂは、暗号処理装置２１０の機能によって、暗号化情報２０７に対称鍵２０３を暗号鍵とした対称鍵復号化を施し、情報２０１を生成する。

【００４５】上記手順によって情報転送元半導第記憶媒体１１０ａから出力された暗号化情報２０７は、対称鍵２０３がないと正当に復号できない。又、暗号化対称鍵２０８は、第２の非対称鍵２０５ｂがないと正当に復号できない。ここで、第２の非対称鍵２０５ｂは、情報転送元半導体記憶媒体１１０ｂ固有の鍵データであり、同機器以外ではこれを得ることができない。従って、暗号化情報２０７の転送経路上に存在する、専用情報処理装置１０５、又は汎用情報処理装置１０６及び半導体記憶媒体アクセス手段１０７、又は再生装置１０８などの機器においては、暗号化対称鍵２０８を復号して情報２０１を利用することができない。

【００４６】又、情報転送元半導第記憶媒体１１０ａと情報転送先半導第記憶媒体１１０ｂ間のデータ転送過程において、暗号化情報２０７の送出と暗号化対称鍵２０８の送出の間の時点で、情報転送元半導第記憶媒体１１０ａ内に存在する情報２０１が無効化される（ステップ６０７）ため、情報転送元半導第記憶媒体１１０ａと情報転送先半導第記憶媒体１１０ｂの両方の装置上に、情報２０１が存在する期間が生じない。これにより、暗号化情報２０７の転送完了時点で、情報２０３を保有する権利は情報転送元半導第記憶媒体１１０ａから情報転送先半導第記憶媒体１１０ｂに移動したとみなすことが可能であり、以降、情報転送元半導第記憶媒体１１０ａは暗号化対称鍵２０８の送出のみを行うことが可能となる。

【００４７】すなわち、情報転送元半導第記憶媒体１１０ａと情報転送先半導第記憶媒体１１０ｂ間のデータ転送過程の任意の時点において、例えば通信エラーや又は悪意の通信遮断による通信の異常終了が生じたとしても、情報転送元半導第記憶媒体１１０ａと情報転送先半導第記憶媒体１１０ｂの双方で情報２０３が利用可能となることがないことを保証できる。

【００４８】尚、本実施例においては、複数の記憶媒体間でデータを移動する例を示したが、必ずしも複数の記憶媒体間でのデータ移動に限る訳ではなく、記憶媒体１１０と、例えば、専用情報処理装置１０５などの記憶媒体以外の機器間で同様の手順に基づいてデータの移動を実現してもよいし、複数の記憶媒体間に複数の情報再生装置１０９又は専用情報処理装置１０５などを介してデータの移動を実現してもよい。

【００４９】又、本実施例においては、暗号化情報の転送（ステップ６０３ａ、６０３ｂ）又は暗号化対称鍵の転送（ステップ６０９ａ、６０９ｂ）において、受信された暗号化情報の転送誤りチェック（ステップ６０４）又は暗号化対称鍵の転送誤りチェック（ステップ６１０）が実行されるとしたが、半導体記憶媒体１１０ａ、１１０ｂと、専用情報処理装置１０５などとの間のデータバス２０９の信頼性が高い場合、該転送誤りチェック処理（ステップ６０４）又は（ステップ６１０）を省略し、暗号化情報受信後すぐに情報受信完転送処理（ステップ６０６ａ、６０６ｂ）、又は暗号化対称鍵２０８受信すぐに非対称鍵復号化（ステップ６１２）の処理を行なってもよい。

【００５０】以上、本実施例における半導体記憶媒体によれば、複数の半導体記憶媒体１１０ａ、１１０ｂ間で、情報２０１の移動が可能であり、且つ同時に複数の半導体記憶媒体１１０ａ、１１０ｂ上で、同一の情報２０１が使用可能となることがないことを保証可能である。すなわち、本実施例における半導体記憶媒体によれ

ば、暗号通信と厳密なトランザクション処理の組み合わせによって、付加価値の高い情報を、複製による不正使用を防ぎながら、記憶媒体間で移動することを可能とした記憶媒体を実現可能である。

【００５１】第１及び第２の実施例においては、暗号処理の実装は、暗号処理装置２１０内の専用のハードウェアによっても、同装置内のＣＰＵとソフトウェア処理によってもよい。又、鍵情報の保管領域、暗号処理に必要なワーク領域は暗号処理装置２１０内に専用に設けても良いし、記憶装置２１１を流用しても良い。

【００５２】また、第１及び第２の実施例においては、情報２０１の暗号化に対称鍵暗号方式、同対称鍵２０３の暗号化に非対称暗号方式を用いる構成を例示したが、必ずしもこの構成に限定するものではなく、情報の暗号化、暗号鍵の暗号化という二段構成を取り、且つ、同暗号鍵を暗号化する鍵を媒体固有に秘密裏に保持することが可能であるならば、用いる暗号方式は、対称鍵暗号方式、非対称鍵暗号方式を任意に組み合わせてよい。

【００５３】第１及び第２の実施例で示した半導体記憶媒体１１０（または１１０ａ、１１０ｂ）は記憶媒体本来の機能である記憶装置２１１とＩ／Ｆ装置２１２に加え、暗号処理装置２１２を具備する。この半導体記憶媒体１１０は外部装置とのやり取り全てをＩ／Ｆ装置２１２のみを介して行い、又、例えば記憶装置２１１、Ｉ／Ｆ装置２１２及び暗号処理装置２１２を同一の半導体ウェハ上に構成することなどにより、上記装置間を接続するデータバス２１３に外部から直接アクセスすることは困難な構成とする。これにより、半導体記憶媒体１１０の記憶装置２１１に記憶された情報２０１や、暗号処理に必要な鍵情報２０３、２０５ａ、２０５ｂに不正にアクセスすることを防止し、耐タンパ性能を高める。

【００５４】また、第１及び第２の実施例で示した半導体記憶媒体１１０の実現形態としては、例えば、フラッシュメモリを記憶装置２１１とし、暗号処理装置２１０、Ｉ／Ｆ装置２１２を同一の半導体ウェハ上に構成した半導体チップを、例えば切手やクレジットカード程度の大きさのパッケージに封止したものが考えられる。上記形態の半導体記憶媒体１１０を情報流通媒体とすることで、図１に示したような情報処理システム上で高付加価値情報をユーザが利用する際の利便性を向上させることが可能である。

【００５５】又、第１及び第２の実施例では記憶装置２１１として何らかの半導体記憶装置を用いた半導体記憶媒体について示したが、必ずしも半導体記憶媒体に限定するものではなく、例えば、記憶装置として磁気記憶装置を用いた磁気記憶媒体としても問題はない。この場合、例えば、暗号処理装置２１０、Ｉ／Ｆ装置２１２、磁気記憶装置へのアクセス手段を同一の半導体ウェハ上に構成することで、データバス２１３への記憶媒体１１０外からのアクセスを防ぐことが可能である。

【００５６】又、上記第１又は第２の実施例においては、半導体記憶媒体１１０を図２又は図５に示す構成としたが、これを図７に示す構成としてもよい。

【００５７】図７は半導体記憶媒体の他の実施例を示す概略構成図であり、第１又は第２の実施例に用いることができる。図において、図２または図５に示す構成要素と同じものには同一の符号を付し、その説明を省略する。図において、２１２ａは、半導第記憶媒体１１０と外部機器との間で通常のデータ及び制御信号のやり取りを制御するデータインターフェース装置（以下、データＩ／Ｆ装置）である。２１２ｂは、半導第記憶媒体１１０と外部機器との間で安全に交換すべきデータ及び制御信号のやり取りを制御するデータインターフェース装置（以下、セキュアデータＩ／Ｆ装置）である。

【００５８】２０９ｃは、半導第記憶媒体１１０と外部機器間で通常のデータ及び制御信号をやり取りするデータバスである。２０９ｄは、半導第記憶媒体１１０と外部機器間で安全に交換すべきデータ及び制御信号をやり取りするセキュアデータバスである。記憶媒体１１０外部から見えるＩ／Ｆ装置を物理的に複数具備し、例えば、第１の非対称鍵２０５ａや第２の非対称鍵２０５ｂの記憶装置２１１への設定や、ここでは方式の詳細は述べないが記憶媒体１１０、外部装置間の認証手続きなど、システムの安全上特に重要な情報のやり取りについては、セキュアデータＩ／Ｆ装置２１２ａを介して行う。暗号化情報２０７の送受信など特に重要ではないものについては、データＩ／Ｆ装置２１２ｂを介して行う。

【００５９】上記構成によれば、半導第記憶媒体１１０に物理的に独立した複数のデータＩ／Ｆを設けることで、安全上特に重要な情報のやり取りに特化したプロトコルやバス構成を、通常の情報のやり取りとの依存関係なしに定義可能となる。

【００６０】以上説明したように、本発明によれば、情報生成者又は情報生成装置と、情報配信装置と、情報を配信する通信回線と、半導体記憶媒体と、該通信回線と接続され該半導体記憶媒体に情報を書き込む端末と、通信回線とは独立した状態で半導体記憶装置に格納されている情報を再生する情報再生装置からなる系において、記憶媒体に格納されている情報を他の情報機器又は記憶媒体で使用することが不可能な形式で出力することが可能な記憶媒体及びそれを用いた情報処理システムを提供することと、記憶媒体に格納されている情報を複製ではなく移動することで、情報の唯一性を保証することが可能である。

【００６１】これにより、付加価値の高いデータも安全に半導体記憶媒体で流通させることが可能となり、情報配信サービスなどへの応用が可能となる。

【００６２】

【発明の効果】以上説明したように、本発明によれば、

記憶媒体に格納されている情報を他の情報機器又は記憶媒体で使用することが不可能な形式で出力することが可能である。また、記憶媒体に格納されている情報を複製ではなく移動することで、情報の唯一性を保証することが可能である。これにより、付加価値の高いデータも安全に半導体記憶媒体で流通させることが可能となり、情報配信サービスなどへの応用が可能となる。

【図面の簡単な説明】

【図１】本発明を適用することができる情報処理システムの一実施例の概要を示すブロック図である。

【図２】本発明による記憶媒体の第１の実施例を示す構成図である。

【図３】本発明による情報移動システムの記憶媒体からの情報転送機能の第１の実施例を示す図である。

【図４】本発明による情報移動システムの記録媒体への情報転送機能の第１の実施例を示す図である。

【図５】本発明による情報管理及び移動システムの概略構成図である。

【図６】本発明による情報移動システムの第２の実施例の動作を示すフローチャートである。

【図７】半導体記憶媒体の他の実施例を示す概略構成図である。

【図８】図３の情報移動システムの動作を説明するためのフローチャートである。

【図９】従来の複製による不正使用防止システムを示すブロック図である。

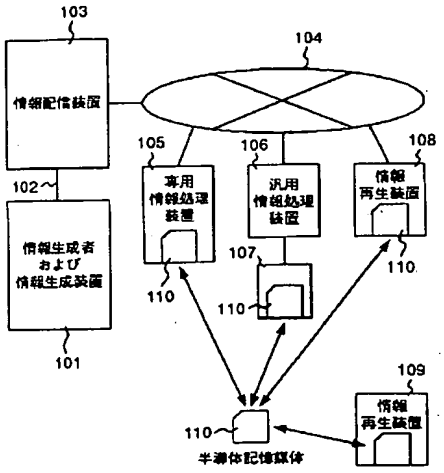
【図１０】従来の情報移動システムのフローチャートである。

【符号の説明】

１０１…情報生成者および情報生成装置、１０２…転送手段、１０３…情報配信装置、１０４…通信回線、１０５…専用端末、１０６…汎用情報処理装置、１０７…半導体記憶媒体アクセス手段、１０８…情報再生装置、１０９…情報再生装置、１１０…半導体記憶媒、２０１…情報、２０２…対称鍵生成処理、２０３…対称鍵、２０４…対称鍵暗号処理、２０４ａ…対称鍵暗号化処理、２０４ｂ…対称鍵復号化処理、２０５ａ…第１の非対称鍵、２０５ｂ…第２の非対称鍵、２０６…非対称鍵暗号処理部、２０６ａ…非対称鍵暗号化処理、２０６ｂ…非対称鍵復号化処理、２０７…暗号化情報、２０８…暗号化対称鍵、２０９…データバス、２０９ａ…暗号化情報、暗号化対称鍵送信、２０９ｂ…暗号化情報、暗号化対称鍵受信、２０９ｃ…データバス、２０９ｄ…セキュアデータバス、２１０…暗号処理装置、２１１…記憶装置、２１２…Ｉ／Ｆ装置、２１２ａ…データＩ／Ｆ装置、２１２ｂ…セキュアデータＩ／Ｆ装置、５０１ａ…Ｉ／Ｆ装置、５０１ｂ…Ｉ／Ｆ装置、５０２…制御装置、５０３ａ…データバス、５０３ｂ…データバス、６０１…対称鍵生成処理、６０２…対称鍵暗号化処理、６０３ａ…暗号化情報送信、６０３ｂ…暗号化情報受信、６０４…暗号化情報鍵の転送誤りチェック処理、６０５ａ…情報再送要求送信、６０５ｂ…情報再送要受信、６０６ａ…情報受信完送信、６０６ｂ…情報受信完受信、６０７…情報の削除処理、６０８…非対称鍵暗号化処理、６０９ａ…暗号化対称鍵送信、６０９ｂ…暗号化対称鍵受信、６１０…暗号化対称鍵の転送誤りチェック処理、６１１ａ…対称鍵再送要求送信、６１１ｂ…対称鍵再送要求受信、６１２…非対称鍵復号化処理、６１３…対称鍵復号化処理、９０１…ネットワーク、９０２…クライアント、９０３…音楽配信サーバ、９１０…パーソナルコンピュータ、９１１…携帯用ヘッドフォンステレオ、９２２…音楽データベース。

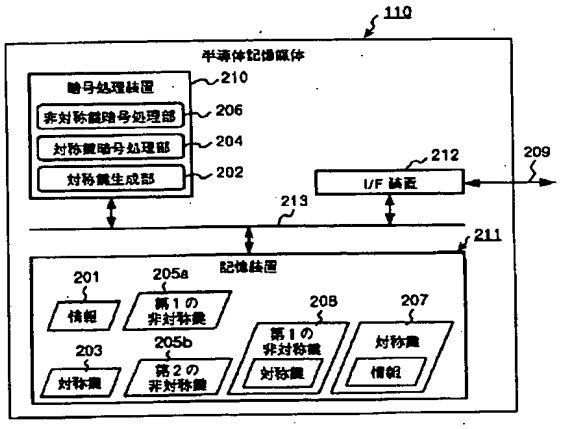
【図１】

図　1



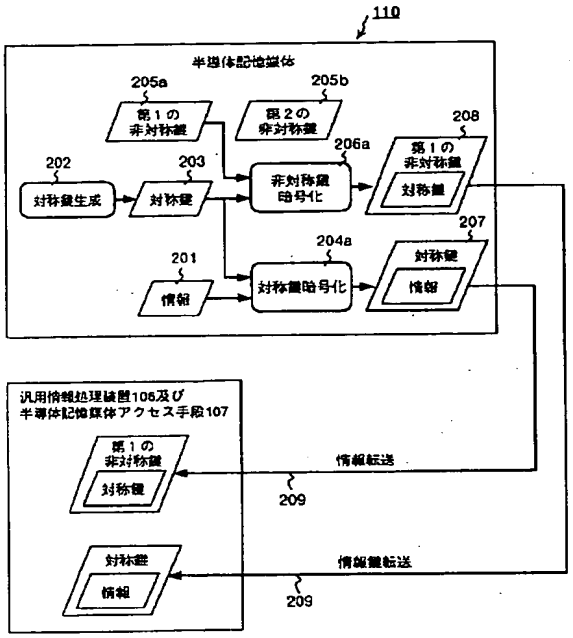
【図２】

図　2



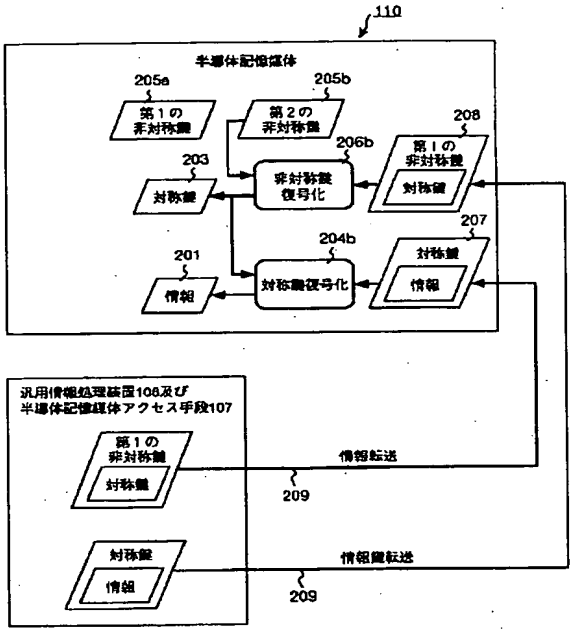
【図３】

図 3



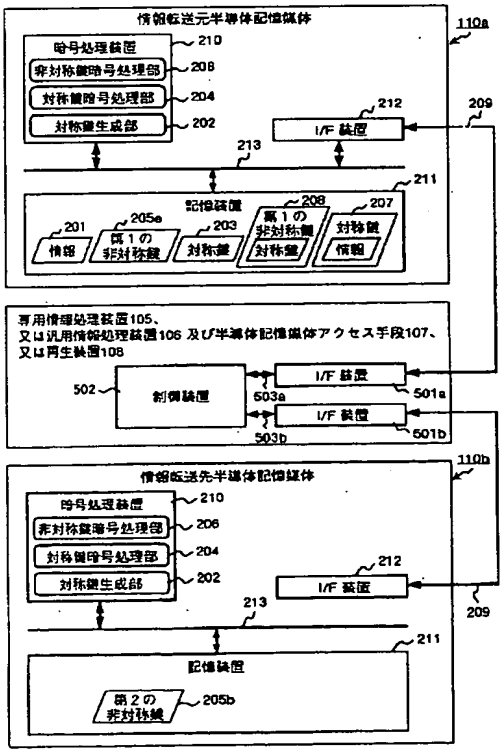
【図４】

図 4



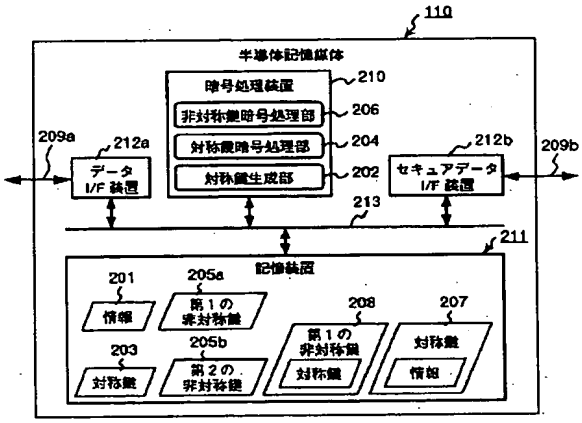
【図５】

図 5



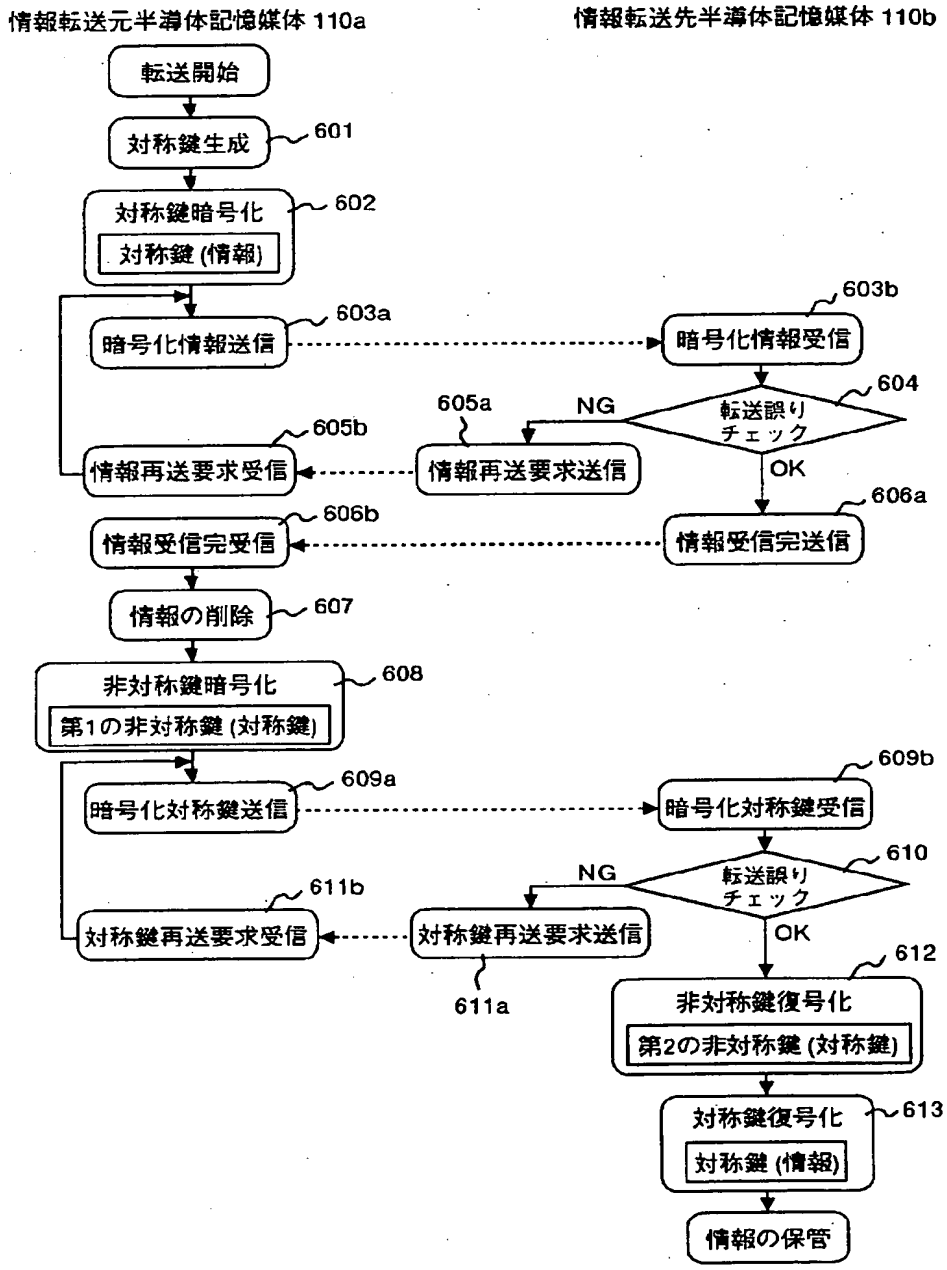
【図７】

図 7



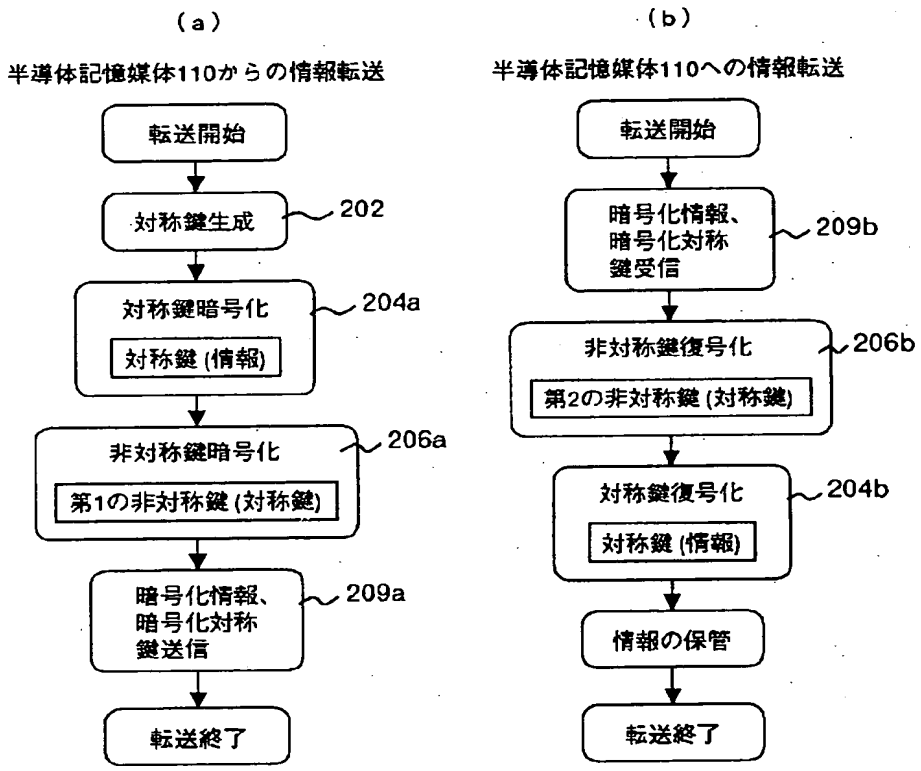
【図６】

図　6


情報転送元半導体記憶媒体 110a
情報転送先半導体記憶媒体 110b
転送開始
対称鍵生成
601
対称鍵暗号化
対称鍵 (情報)
602
暗号化情報送信
603a
暗号化情報受信
603b
転送誤り
チェック
604
NG
605a
OK
情報再送要求受信
605b
情報再送要求送信
情報受信完受信
606b
情報受信完送信
606a
情報の削除
607
非対称鍵暗号化
第1の非対称鍵 (対称鍵)
608
暗号化対称鍵送信
609a
暗号化対称鍵受信
609b
転送誤り
チェック
610
NG
OK
対称鍵再送要求受信
611b
対称鍵再送要求送信
611a
非対称鍵復号化
第2の非対称鍵 (対称鍵)
612
対称鍵復号化
対称鍵 (情報)
613
情報の保管

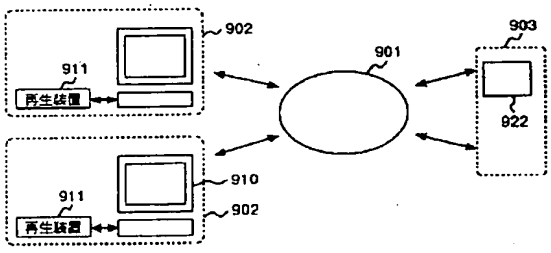
【図８】

図　8


（ａ）
半導体記憶媒体110からの情報転送
転送開始
対称鍵生成
202
対称鍵暗号化
対称鍵（情報）
204a
非対称鍵暗号化
第1の非対称鍵（対称鍵）
206a
暗号化情報、
暗号化対称
鍵送信
209a
転送終了
（ｂ）
半導体記憶媒体110への情報転送
転送開始
暗号化情報、
暗号化対称
鍵受信
209b
非対称鍵復号化
第2の非対称鍵（対称鍵）
206b
対称鍵復号化
対称鍵（情報）
204b
情報の保管
転送終了

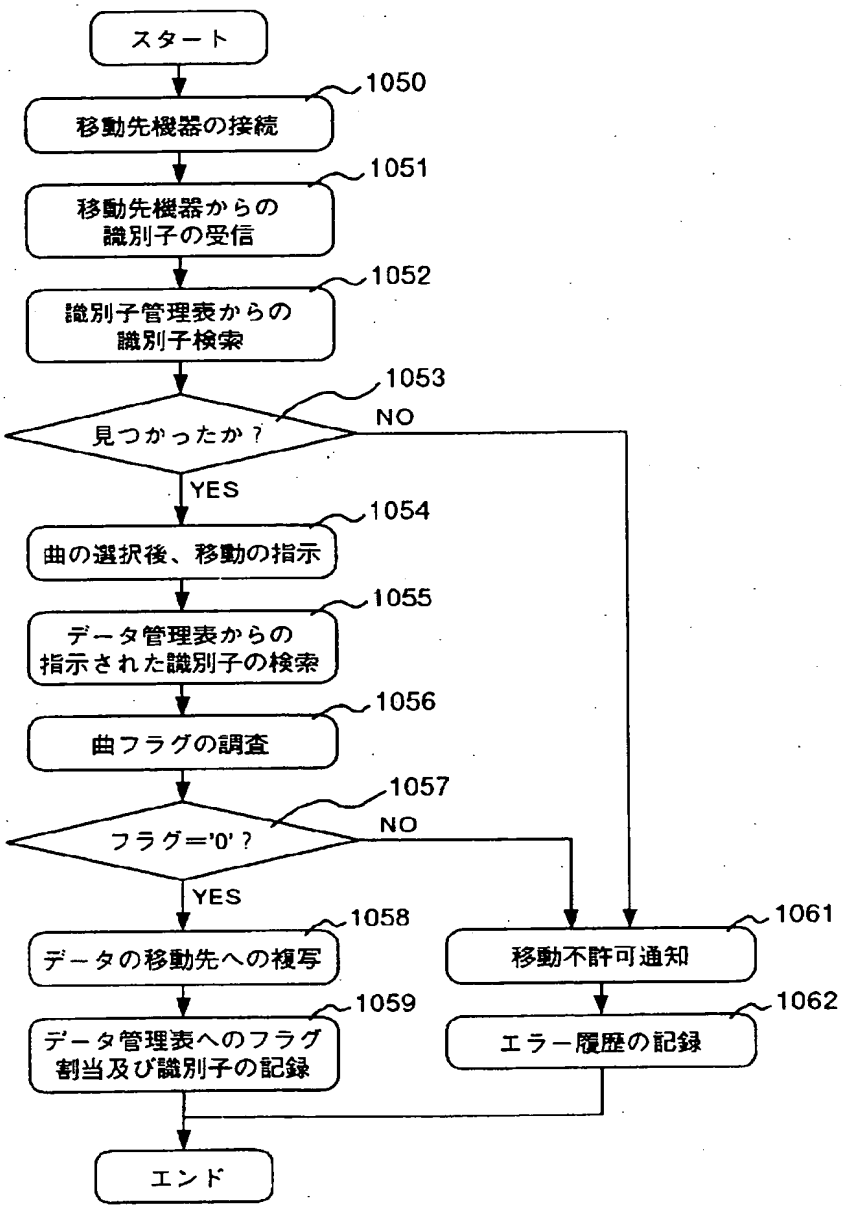
【図９】

図　9


902
911
再生装置
901
903
922
910
902
911
再生装置

【図１０】

図　１０



フロントページの続き

(72)発明者　朝日　猛
神奈川県川崎市麻生区王禅寺1099番地　株式会社日立製作所システム開発研究所内

(72)発明者　田村　隆之
神奈川県川崎市麻生区王禅寺1099番地　株式会社日立製作所システム開発研究所内

(72)発明者　水島　永雅
神奈川県川崎市麻生区王禅寺1099番地　株式会社日立製作所システム開発研究所内
(72)発明者　川崎　郁也
東京都小平市上水本町五丁目20番１号　株式会社日立製作所半導体グループ内
(72)発明者　戸塚　隆
東京都小平市上水本町五丁目20番１号　株式会社日立製作所半導体グループ内

Ｆターム(参考)　5B017 AA06 BA07 CA16
5J104 AA13 AA16 EA04 EA19 EA22
JA03 NA02 NA35 NA37 NA42